Amendments to the Specification:

Please amend the specification as follows:

On page 11, before line 13, please insert the following paragraphs:

Fig. 1 illustrates the basic invention of creating and restyle-linking virtual chip cards. In Fig. 1 the reference numeral 10 designates a chip card communicating with a communication device 12. A number of points of contact constituted by virtual chip cards 14 are connected to PRPs (Privacy Reference Points) 16. Parts of the PRPs are connected to ID units 18, and parts of the ID units 18 together with the PRPs not connected to the ID units 18 are connected to an anonymizer and mixnet 20. The anomymizer/mixnet 20 and the ID units 18 not connected to the anonymizer/mixnet 20 are connected to a home communication device 24, including a home chip card 22.

Fig. 2 illustrates the linking between the product life cycle in the commercial value chain and how the product transfers to consumer privacy control and then eventually re-enters the product life cycle for recycling of materials, etc. In Fig. 2 the communication device 20 with the chip card 10 are shown, as is a store 28 receiving products from a producer supply chain 26 and delivering products to a product recycling function/apparatus 40. An anonymizer/mixnet/ID service 36 communicates through a PRP 30 with the store 28. The anonymizer/mixnet/ID service 36 further communicates with a home chip card 38. The solid line signature 32 represents a product tag visible, and the dotted line signature 34 designates product tag privacy enabled through zero-knowledge device authentication.

On page 27, after line 20, please insert the following paragraphs:

Fig. 9 illustrates how the solution is extended in one embodiment by direct management of personal identities using wireless or other personal communication devices. The chip card 10 is communicating, as indicated by the reference numeral 56, with a card reader 20 which further communicates, as indicated by the reference numeral 58, with a shop computer 44. The card reader 20 further communicates, as indicated by the reference numeral 60, with a service provider further communicating, as indicated by the reference numeral 62, with a financial credential institution 52 and with an identity provider 54, as indicated by the reference numeral

64. The identity provider 54 and the financial credential institution 52 are communicating with one another, as indicated by the reference numeral 68. The service provider 46 and identity provider 54 are further communicating with one another through a mixnet 50, and the identity provider 54 is communicating with a client 48, as indicated by the reference numeral 66, as the client 48 is still further communicating with the chip card 10, as indicated by the reference numeral 49.

Fig. 10 illustrates the device authentication according to the present invention. Fig. 10 illustrates schematically the separation, as indicated by a solid line between the home/trusted space including MADs (Master Authentication Devices), MCDs (Master Communication Devices), SMDs (Specific Master Devices) and SDs (Slave Devices) and the ID Mixnet in which communication is based on pure pseudonyms and no direct device access is established. The ID mixnet further communicates with standard PRP processes device zero-knowledge/device only known at point of purchase devices, VDRs, i.e. Virtual Device References, in which each virtual device includes different key, and no re-use is made between the boundaries. In the system the manufacturer can verify new hardware-based VDRs using blinded signatures and credentials, and the system still further includes group privacy device authentications using one-time-only tickets.

Fig. 11 illustrates privacy-managed digital signatures with instant revocability and shows the chip card 10 and the communication device 12. The virtual chip cards 14 are further shown communicating with the PRPs (Privacy Reference Points) 16. From the PRPs 16 communication is established to the mixnet. The reference numeral 74 indicates a CA/signature unit, the reference numeral 76 indicates an access one-time-only encrypted copy of a signature decryption key, and the reference numeral 78 indicates "If authenticated a chip card not revoked" return data. The reference numeral 80 indicates optional server side support, and the reference numeral 82 designates a forward signature.

In Fig. 12 the basic infrastructure per privacy enabled RFID using untrusted RFID and chip card readers is shown, as the reference numeral 10 designates the chip card communicating, as indicated by the reference numeral 56, with the card reader 42, which further, as described above, communicates with the service provider 46, as indicated by the reference numeral 60. The card reader 42 further communicates with an RFID reader 88, as indicated by the reference

numeral 94, which RFID reader communicates, as indicated by the reference numeral 90, with an RFID chip 84. The RFID reader 88 further communicates, as indicated by the reference numeral 92, with the shop computer 44, and also communicates, as indicated by the reference numeral 110, with the card reader 42 and with the supplier 86.

On page 37, after line 29, please insert the following paragraphs:

Fig. 14 illustrates how to create private proximity ticket using a combination of group authentication and PRPs. Fig. 14 shows a home computer 102, an RFID reader 124, a mixnet 118, and a shop computer 122. The communication between the home computer 102 and the shop computer 122 is designated the reference numeral 100. The shop computer 122 further communicates, as indicated by the reference numeral 98, with an event 130 which is governed by an RFID reader 128. The RFID reader 128 communicates, as indicated by the reference numerals 108, 110 and 114, with a portable proximity RFID tag 126 from which communication is further established to the home computer 102, as indicated by the reference numeral 106. Centrally, within the system, a PRP service provider 120 is included. The communication from the home computer 102 to the PRP is indicated by the reference numeral 104, and the communication from the RFID reader 128 to the PRP is designated the reference numeral 112.

Fig. 15 illustrates how to create connection between anonymous sessions. The reference numeral 1 designates a PRP provider. The reference numeral 132 designates a mobile unit A, the reference numeral 134 designates a channel provider A, and the reference numeral 136 designates an instant messaging provider A. Similarly, the reference numeral 142 designates a unit B, the reference numeral 144 designates a channel provider B and the reference numeral 146 designates an instant messaging provider B. The reference numerals 138 and 148 designate the communication from the mobile unit A 132 and the unit B 142, respectively, to the channel provider A 134 and the channel provider B 144, respectively. The reference numerals 150 and 160 designate privacy reference points with which the channel provider A 134 and the channel provider B 144 communicate, as indicated by the reference numerals 152 and 162, respectively. Communication between the mobile unit A 132 and the unit B 142 is indicated by the reference numeral 172 through a communication block 170.

Fig. 16 illustrates a zero-knowledge authentication process including group authentication and device authentication. Fig. 16 illustrates in plain text the generic tag authentication.

Fig. 17 illustrates a mobile device able to directly control the personal space. In Fig. 17 the chip card 10 is shown together with the card reader 42 centrally within a mobile privacy system that also includes centrally an RFID reader 88 and a wireless communication 176. As shown in Fig. 17, a supplier 86 having a shop computer 44 communicates with the RFID reader 88 and an RFID chip 84. Through communication links indicated by the reference numerals 90 and 58, the RFID chip 84 communicates with the RFID reader 88, and the shop computer 44 communicates with the central system including the card reader 42. The shop computer 44 further communicates with a service provider 46, which communicates with an identity provider 178 connected with a channel provider 180 and a digital key 182 of a mobile client unit.

Please replace the paragraph beginning on page 41, line 15 with the following rewritten paragraph:

One aspect of RFID authenticity is the ability to improve authentication of Identity devices such as a ~~MAD device~~ master authentication device (MAD) incorporating a secure chip card combined with the ability to communicate. User authentication towards the MAD is based on passwords, having the physical device, biometrics towards templates etc. and can be augmented with a RFID Tag that the MAD ~~require~~ requires to be nearby. The MAD authenticates towards the MAD which then [[try]] tries to detect a specific RFID Tag nearby which can be worn by the owner or even surgically implanted. When context is established the end-user can create a context-specific dynamic session key for re-authentication and define its limitation in time and access rights. This way the enduser can define balances between security, tracking and convenience varying from application to application.